Lampi di Cassandra/ Il Signore dei laptop

(323)—Dal Trusted Computing all'hardware dedicato al monitoraggio, infilato nei chipset per garantire tutti i benefici…

Lampi di Cassandra/ Il Signore dei laptop

Figure 1:

(323)—Dal Trusted Computing all'hardware dedicato al monitoraggio, infilato nei chipset per garantire tutti i benefici dell'amministrazione remota. E non solo.

Figure 2:

> "Un Chipset per domarli, Un Chipset per trovarli,
>
> Un Chipset per ghermirli e nel buio incatenarli."

Le parole di Sauron mentre l'Unico Anello viene forgiato possono essere facilmente adattate all'ultima creazione della più grande "fonderia" di CPU e chipset del mondo.

Nessun raptus di paranoia, solo ricorrenti news tecnologiche che sono ormai di casa in questa rubrica, ultima tra tutte quella che discuteva i problemi derivanti dai BIOS contenenti il

prodotto Computrace, in grado di caricare ed attivare programmi all'interno del sistema operativo, anche se il disco venisse riformattato.

Il problema di fondo è ormai notissimo, ed è costituito dal crescente numero di funzionalità nascoste all'utente che risiedono nell'hardware/firmware dei nuovi computer, ed in particolare quelle cosiddette di amministrazione remota.

Chi l'avrebbe detto? Per anni ci siamo preoccupati del Trusted Computing con le sue barriere crittografiche, ed invece presto ci troveremo semplicemente con dell'hardware di monitoraggio inserito in maniera ineliminabile in tutti i laptop e pc di ultima produzione.

Uno fra gli ultimi chipset di Intel viene così descritto dal blog Popular Resistance: "*…Core vPro processors work in conjunction with Intel's new Anti Theft 3.0, which put 3g connectivity into every Intel CPU after the Sandy Bridge version of the I3/5/7 processors. Users do not get to know about that 3g connection, but it is there*".

Chi volesse i dettagli del ben documentato articolo potrà approfondirli, ma a Cassandra preme semplificare e riassumere.Un chipset è l'insieme di circuiti integrati che insieme alla CPU sono i componenti attivi che permettono ai fabbricanti di pc o laptop di progettare e costruire un nuovo modello.

Tutti usano gli stessi chipset, che sono disponibili in poche famiglie diverse.La prossima di queste porterebbe molto più avanti il concetto di "amministrazione remota", cioè quella lodevole funzionalità che permette, in una grande azienda, di far svolgere le operazioni di assistenza e ricerca guasti via rete. I primi pc dotati di questa funzionalità, ed assai più costosi di quelli normali, avevano una seconda presa di rete che permetteva di gestire la componentistica di accesso remoto. Se non la collegavate ad un cavo di rete non poteva essere utilizzata.

I più recenti chipset usano la normale scheda di rete, ed integrano tutto nel silicio rendendolo non rimovibile.Cosa può fare l'amministratore che acceda via rete un laptop dotato del "prossimo chipset"?

Se la batteria o l'alimentazione sono collegate, potrà utilizzarlo anche se il laptop è spento, eseguendo qualsiasi operazione sia alla portata del sistema operativo, più operazioni "diagnostiche" che nemmeno il sistema operativo può svolgere.

Il laptop è acceso ed in uso? Meglio, potrà anche monitorare ed amministrare il sistema operativo senza che l'utente si accorga di niente. Potrebbe anche leggere l'hard disk criptato e recuperare le chiavi crittografiche smarrite, visto che potrà registrarle al momento della generazione.

Ma se la rete è scollegata ed il WiFi non è attivo? Nessun problema, visto che il prossimo chipset potrà collegarsi via rete cellulare 3G, senza contratti ed anche da spento.

E se l'hard disk, ed ogni altro supporto di memoria flash fosse guasto o venisse scollegato fisicamente? Malgrado questo il chipset, che possiede un suo sistema operativo, può continuare a lavorare e fare cose lodevoli, come per esempio attivare il microfono o la telecamera incorporati per aiutare l'utente.

E se il guasto interessa la RAM e l'avete anche tolta per vedere la sigla e ricomprarla? Siete fortunati lo stesso, il chipset ha la sua RAM e continua a lavorare tranquillamente. Il vostro amministratore remoto potrà continuare ad aiutarvi vostro malgrado. Speriamo però che l'NSA non lo venga mai a sapere: cosa non potrebbe fare con queste nuove funzionalità…

Beh, ma perché scomodarli: chiunque sia abituato a fare un po' di hacking potrebbe usarle. Anzi, più un hardware è insicuro, minore è la sicurezza per tutti, dai possessori di pc fino

all'NSA stessa. E pur non essendo i Russi lettori di Cassandra (almeno non credo), anche loro sembrano avere qualche dubbio in proposito, visto che notizie insistenti riferiscono della volontà di non acquistare più computer basati su chipset Intel/AMD ma costruirseli completamente in casa.

Tenete perciò di conto il vostro hardware vintage: un domani potrebbe valer dei soldi ed esservi anche molto, molto utile.

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

***Licenza d'utilizzo**: i contenuti di questo articolo, dove non diversamente indicato, sono sotto licenza Creative Commons Attribuzione—Condividi allo stesso modo 4.0 Internazionale (CC BY-SA 4.0),* tutte le informazioni di utilizzo del materiale sono disponibili a questo link.

By Marco A. L. Calamari on April 8, 2023.

Canonical link

Exported from Medium on August 27, 2025.